THE DISTRICT COURT OF THE UNITED STATES

for the Western District of New York

THE UNITED STATES OF AMERICA

-vs-

RYAN JAMES ROACH
(Counts 1–3), and

MATHIEW JAMES STUBBINGS
(Counts 1–3)

April 2022 GRAND JURY
(Impaneled April 29, 2022)

INDICTMENT

Violations:
Title 18, United States Code, Sections 371, 1030(a)(2)(C), 1030(a)(5)(A), and 2
(3 Counts and 2 Forfeiture Allegations)

COUNT ONE

(Conspiracy to Obtain Information from a Protected Computer and to Cause Damage to a Protected Computer)

The Grand Jury Charges That:

Overview

At all times material to this Indictment, unless otherwise alleged:

1. The Defendants, RYAN JAMES ROACH ("ROACH") and MATHIEW JAMES STUBBINGS ("STUBBINGS"), were engaged in a scheme to hack into computers, steal login credentials, and secretly mine cryptocurrency.

2. To effectuate the scheme, the Defendants used virtual private servers in multiple countries, which were registered under false names. These servers transmitted malware and mining software to victim computers and stored stolen login credentials.

3. Victims of the scheme included educational institutions in New York, Tennessee, North Carolina, and Massachusetts. Some of the computers damaged by the Defendants were in the Western District of New York.

4. The Defendants accessed protected computers without authorization for private financial gain. As a result of the scheme, the Defendants damaged ten or more protected computers during a one-year period. The Defendants also caused an aggregate loss of at least $5,000 to persons during a one-year period, resulting from a related course of conduct that affected one or more other protected computers.

The Defendants

5. ROACH was a citizen and resident of Canada.

6. STUBBINGS was a citizen and resident of Canada.

Victims

7. Victims of the scheme, the identities of which are known to the Grand Jury, included:

a. Institution 1: an institution of higher learning located in the Western District of New York.

b. Institution 2: an institution of higher learning located in the Eastern District of Tennessee.

c. Institution 3: an institution of higher learning located in the Eastern District of North Carolina.

d. Institution 4: an institution of higher learning located in the District of Massachusetts.

Relevant Entities

8. European VPS #1 was a virtual private server hosted in Europe.

9. European VPS #2 was a virtual private server hosted in Europe.

10. US VPS #1 was a virtual private server hosted in the United States.

Definitions

11. A "network" was a group of two or more computers that were linked together for the purpose of communicating data electronically.

12. A "server" was a type of computer on a network that managed network resources.

13. A "supercomputer," also known as a high-performance computer, was a computer (or a series of computers) with massive computational power compared to a general-purpose computer. Supercomputers were used by researchers at higher-level institutions for projects that involved large volumes of data or required significant computational power.

14. A "virtual private server" ("VPS") was the emulation of a physical server through software. A VPS functioned like a physical server: it had its own operating system and private allocation of resources. Among other things, a VPS could be used to transmit files, store information, and browse the Internet.

15. "Malware" was malicious software that was installed on a computer without the knowledge or permission of the computer's owner. Malware could be used for a variety of purposes, including to log another user's keystrokes, to transfer control of the computer to another person, and to bypass computer restrictions in order to install additional software.

16. A "rootkit" was a type of malware that gave a person continuous, unauthorized access to a computer without being detected.

17. A "bullet-proof host" was an online service provider from which law enforcement supposedly could not gain access or obtain information.

18. A "cryptocurrency" was a digital currency that was circulated over the Internet. Encryption techniques, known as cryptography, were used to regulate the generation of units of cryptocurrency and validate cryptocurrency transfers. Examples of cryptocurrencies included Bitcoin, Electroneum, and Sumokoin.

19. "Cryptocurrency addresses" were virtual locations to which cryptocurrencies were sent and received—for example, a transfer of Bitcoin to a Bitcoin address. A cryptocurrency address was analogous to a bank account number and was represented by a case-sensitive string of letters and numbers. Each address was controlled by a unique corresponding private key, which was the equivalent of a password needed to access the address. Only the holder of an address' private key could authorize transfers of cryptocurrency from that address.

20. "Cryptomining," also known as the "mining" of cryptocurrency, was the use of a computer to solve the mathematics behind the generation of a cryptocurrency or the

validation of cryptocurrency transactions. The solver of the mathematical problem was generally compensated with a small amount of new cryptocurrency (in the case of the initial generation of currency) or a small percentage of the validated cryptocurrency transaction.

The Conspiracy

21. From on or about June 1, 2016, to in or about December 2019, in the Western District of New York, and elsewhere, the Defendants, RYAN JAMES ROACH and MATHIEW JAMES STUBBINGS, did knowingly and intentionally conspire and agree to commit offenses against the United States, that is:

a. to intentionally access a computer without authorization, and thereby obtain information from a protected computer, for the purpose of private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i); and

b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to one or more persons during a one-year period aggregating at least $5,000 in value resulting from a related course of conduct affecting one or more other protected computers, and cause damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B).

Objectives of the Conspiracy

22. The objectives of the conspiracy were for the Defendants to enrich themselves by:

a. conducting research to select and target potential victims;

b. surreptitiously accessing victims' computers without authorization;

c. deploying malware to gain control of victims' computers;

d. stealing victims' login credentials and exfiltrating the data to servers controlled by the Defendants; and

e. forcing victim computers to use their processing power to mine cryptocurrency for the financial benefit of the Defendants.

Manner and Means of the Conspiracy

23. The manner and means used to accomplish the conspiracy's objectives included the following:

a. The Defendants rented European VPS #1, European VPS #2, and US VPS #1 under false names.

b. The Defendants registered cryptocurrency addresses and obtained software to mine those cryptocurrencies.

c. The Defendants identified potential victims—such as educational institutions in the United States that had supercomputers—and researched security vulnerabilities in the victims' computer networks.

d. The Defendants hacked into (*i.e.*, accessed without authorization) the computer networks of victims. The Defendants used a variety of methods to gain access to victim networks, including using US VPS #1 and compromised computers from another victim to conceal their identities.

e. Once inside a victim's network, the Defendants used sophisticated techniques and tools to conduct reconnaissance and expand their access within the network. For instance, the Defendants used European VPS #1 to transmit a rootkit to a victim's network.

f. The Defendants also stole victim login credentials and exfiltrated the data to servers controlled by the Defendants, such as European VPS #1 and US VPS #1.

g. The Defendants used servers such as European VPS #1 to transmit mining software to victim computers. The Defendants caused at least one supercomputer to mine cryptocurrency on their behalf, which caused much of the supercomputer's processing speed and power to become unavailable to its legitimate owner.

Overt Acts

24. In furtherance of the conspiracy and to achieve its objectives, the Defendants committed and caused to be committed the following overt acts in the Western District of New York and elsewhere:

a. In or about June 2016, Defendant ROACH provided Defendant STUBBINGS with authorization to pay for US VPS #1.

b. In or about May 2017, Defendant ROACH used an online search engine to research how to identify confidential informants.

c. In or about August 2017 and September 2017, Defendant ROACH used an online search engine to research bullet-proof hosts located overseas.

d. In or about September 2017, the Defendants registered European VPS #1.

e. In or about September 2017, Defendant ROACH used an online search engine to research computer vulnerabilities and hacking.

f. In or about October 2017, Defendant STUBBINGS attempted to purchase computer vulnerabilities.

g. From on or about October 9, 2017, to on or about November 1, 2017, the Defendants used European VPS #1 to transmit malware and mining software to computers at Institution 2.

h. From on or about October 13, 2017, to on or about October 29, 2017, the Defendants used European VPS #1 to transmit malware and mining software to computers at Institution 3.

i. On or about November 1, 2017, Defendant ROACH used an online search engine to research high-performance computing at Institution 1.

j. On or about November 1, 2017, the Defendants used European VPS #1, European VPS #2, and a compromised victim computer to access Institution 1's computer network without authorization.

k. On or about November 1, 2017, the Defendants used European VPS #1 to transmit malware files to computers at Institution 1. Among other things, the malware provided the Defendants with expanded access to Institution 1's network and recorded the keystrokes of users at Institution 1.

l. On or about November 1, 2017, the Defendants copied login credentials and other files associated with users at Institution 1. The Defendants transferred the data to European VPS #1 and US VPS #1.

m. On or about November 1, 2017, the Defendants accessed Institution 1's supercomputer and installed a rootkit.

n. On or about November 1, 2017, Defendant ROACH used an online search engine to research Electroneum mining.

o. On or about November 1, 2017, the Defendants used Institution 1's supercomputer to mine Electroneum, with the proceeds designated to an address controlled by Defendant STUBBINGS. Subsequently,

Institution 1 received reports that its supercomputer was running slowly and terminated the mining software.

p. On or about November 2, 2017, the Defendants again used Institution 1's supercomputer to mine Electroneum, which caused Institution 1 to take its supercomputer offline for a full forensic review.

q. On or about November 3, 2017, Defendant STUBBINGS used a home Internet account to download malware files from European VPS #1. Subsequently, European VPS #1 transmitted the malware to Institution 1.

r. From on or about November 10, 2017, to on or about November 14, 2017, Defendant ROACH used an online search engine to research how to delete server logs.

s. In or about December 2018, Defendant STUBBINGS solicited help to develop a rootkit.

t. In or about June 2019, Defendant STUBBINGS used US VPS #1 to access the computer network of Institution 4 and deploy malware, all without authorization.

u. From an unknown date to at least in or around June 2019, the Defendants used US VPS #1 to store login credentials obtained from Institution 1, Institution 2, Institution 4, and other educational institutions.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

(Obtaining Information from a Protected Computer)

The Grand Jury Further Charges That:

1. The allegations contained in paragraphs 1 through 20, 23, and 24 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. Between on or about October 31, 2017, and on or about November 3, 2017, in the Western District of New York, and elsewhere, the Defendants, RYAN JAMES ROACH and MATHIEW JAMES STUBBINGS, intentionally accessed a computer without authorization, and aided and abetted each other to do so, and thereby obtained information from a protected computer, and the offense was committed for purposes of private financial gain.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i); Title 18, United States Code, Section 2; and *Pinkerton v. United States*, 328 U.S. 640 (1946).

COUNT THREE

(Intentional Damage to a Protected Computer)

The Grand Jury Further Charges That:

1. The allegations contained in paragraphs 1 through 21, 24, and 25 of Count 1 of this Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. Between on or about October 31, 2017, and on or about November 3, 2017, in the Western District of New York, and elsewhere, the Defendants, RYAN JAMES ROACH and MATHIEW JAMES STUBBINGS, knowingly caused the transmission of a program, information, code, and command, and aided and abetted each other to do so, and, as a result

of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to one or more persons during a one-year period aggregating at least $5,000 in value and resulting from a related course of conduct affecting one or more other protected computers, and caused damage affecting ten or more protected computers during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i); Title 18, United States Code, Section 2; and *Pinkerton v. United States*, 328 U.S. 640 (1946).

FIRST FORFEITURE ALLEGATION

The Grand Jury Alleges That:

Upon conviction of Counts 1 through 3 of this Indictment, the Defendant, RYAN JAMES ROACH, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 981(a)(1)(C), Title 18, United States Code, Section 1030(i), and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting, or derived from, proceeds Defendant ROACH obtained directly or indirectly, as the result of such violations and any personal property that was used or intended to be used to commit or to facilitate the commission of the violations. The property to be forfeited includes, but is not limited to, the following:

A. ELECTRONICS

a. One (1) Western Digital Hard drive labeled DEKX1 and serial number WCATR3289407;

b. One (1) LT05 tape, labeled DEKX2 with serial number C06405001508;

c. Hard drives, HGST Serial number K5HAJ8ND and HGST Serial number K5HASS6D;

d. Derivative evidence Hard Drive K5HAJ8ND;

e. Derivative evidence item created from Hard Drive K5HASS6D;

f. 2TB Western Digital HDD Serial number WCAY01767826;

g. Derivative Evidence Copy of Nuclear Fallout Server;

h. Hard drive containing two NFO Images and Network Traffic;

i. Derivative evidence copy of NFO server;

j. Derivative evidence of NFO network traffic captures;

k. Hard drive containing Nuclear Fallout image raven.img.saved-for-fbi-20190604;

l. Derivative evidence copy of 1B11; and

m. Hitachi Hard drive, 500GB, P/N 0F10381, S/N HN3U8LYB.

All pursuant to Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 981(a)(1)(C), Title 18, United States Code, Section 1030(i), and Title 28, United States Code, Section 2461.

SECOND FORFEITURE ALLEGATION

The Grand Jury Further Alleges That:

Upon conviction of Counts 1 through 3 of this Indictment, the Defendant, MATHIEW JAMES STUBBINGS, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 981(a)(1)(C), Title 18, United States Code, Section 1030(i), and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting, or derived from, proceeds Defendant STUBBINGS obtained directly or indirectly, as the result of such violations and any personal

property that was used or intended to be used to commit or to facilitate the commission of the violations. The property to be forfeited includes, but is not limited to, the following:

A. ELECTRONICS

a. One (1) Western Digital Hard drive labeled DEKX1 and serial number WCATR3289407;

b. One (1) LT05 tape, labeled DEKX2 with serial number C06405001508;

c. Hard drives, HGST Serial number K5HAJ8ND and HGST Serial number K5HASS6D;

d. Derivative evidence Hard Drive K5HAJ8ND;

e. Derivative evidence item created from Hard Drive K5HASS6D;

f. 2TB Western Digital HDD Serial number WCAY01767826;

g. Derivative Evidence Copy of Nuclear Fallout Server;

h. Hard drive containing two NFO Images and Network Traffic;

i. Derivative evidence copy of NFO server;

j. Derivative evidence of NFO network traffic captures;

k. Hard drive containing Nuclear Fallout image raven.img.saved-for-fbi-20190604;

l. Derivative evidence copy of 1B11; and

m. Hitachi Hard drive, 500GB, P/N 0F10381, S/N HN3U8LYB.

All pursuant to Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 981(a)(1)(C), Title 18, United States Code, Section 1030(i), 21 U.S.C. § 853(p), and Title 28, United States Code, Section 2461.

SUBSTITUTE ASSETS PROVISION

If any of the above-described forfeitable property set forth in the First and Second Forfeiture Allegations, as a result of any act or omission of the Defendants, RYAN JAMES ROACH and/or MATHIEW JAMES STUBBINGS:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c) and 18 U.S.C. §§ 982(b) and 1030(i)), to the forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

DATED: Rochester, New York, August 25, 2022.

TRINI E. ROSS
United States Attorney

By: s/RICHARD A. RESNICK
Assistant United States Attorney
United States Attorney's Office
Western District of New York
100 State Street, Suite 500
Rochester, New York 14614
Telephone: (585) 263-6760
Richard.Resnick@usdoj.gov

A TRUE BILL:

s/Foreperson
FOREPERSON